ON THE SUM AND DIFFERENCE OF SQUARES OF PRIMES (II)

PAUL ERDÖS*.

[*Extracted from the Journal of the London Mathematical Society, Vol.* 12, 1937.]

In a previous paper† I proved that, for an infinity of m and n, the equations $m = p^2 - q^2$ and $n = p^2 + q^2$, where p and q are primes, have more than $m^{c_1/\log\log m}$ and $n^{c_2/(\log\log n)^2}$ solutions respectively. The proofs were elementary. In § 1 of this paper I prove that, for an infinity of n, the number of solutions of the equation $n = p^2 + q^2$ is greater than $n^{c_3/\log\log n}$. The argument is very similar to that of I, the principal difference being that it requires Brun's method. I give the proof in detail only where it differs from I.

In § 2 we prove the following theorem, which is a generalization of the result proved in § 1 of I.

Let $r_1 < r_2 < \ldots$ be an infinite sequence of positive integers such that for an infinity of N the number of r's less than or equal to N is greater than $N^{1-(c_4/\log\log N)}$, with $c_4 < \frac{1}{2}\log 2$. Then for an infinity of M the number of solutions of the equation $r_j^2 - r_i^2 = M$ is greater than $M^{c_5/\log\log M}$, where c_5 depends only upon c_4.

The results of this paper were stated in I.

1. As in I, we put $A = 5.13 \ldots p_k$, where k is sufficiently large and the p's are the first k primes of the form $4d+1$. We write $A = a_1 a_2 \ldots a_x$, where x is a sufficiently large absolute constant, to be determined later (in I we had $x = [10 \log\log A]$), and all the a's have at least $[k/x]$ prime factors.

First we prove the following

LEMMA. *There exists an a_i such that the number of primes $p < A^2$ in each of at least $\frac{7}{8}\phi(a_i)$ residue classes* mod a_i *is greater than $A^2/\phi(a_i)(\log A)^2$.*

Proof. Suppose that the lemma is not true. For every a_i we divide the $\phi(a_i)$ residues prime to a_i into two classes. Class 1 contains the residues for which the number of primes in each of them is less than $A^2/\phi(a_i)(\log A)^2$; class 2 contains the other residues. Similarly we divide the primes $p < A^2$ with $p \nmid A$ into two groups: in group I we put those primes which, for at least one a_i, are congruent mod a_i to a residue of class 1, in group II all the other primes.

* Received 6 November, 1936; read 12 November, 1936.

† *Journal London Math. Soc.*, 12 (1937), 133–136.

The number of primes $p \leqslant A^2$ congruent for a fixed modulus a_i to a residue of class 1 is evidently less than $A^2/(\log A)^2$. Hence the total number of primes belonging to group I is less than $A^2 x/(\log A)^2$.

The number of residues mod A belonging for every a_i to class 2 is, in consequence of the multiplicativity of the residue classes, less than

$$\tfrac{7}{8}\phi(a_1)\,\tfrac{7}{8}\phi(a_2)\ldots\tfrac{7}{8}\phi(a_x) = (\tfrac{7}{8})^x\,\phi(A).$$

Now, by a theorem due to Brun and Titchmarsh*, the number of primes belonging to group II is less than

$$(\tfrac{7}{8})^x\,\phi(A)\,\frac{c_6 A^2}{\phi(A)\log A} = (\tfrac{7}{8})^x\,\frac{c_6 A^2}{\log A}.$$

But then the number of primes $p \leqslant A^2$ would be less than

$$2\log A + \frac{A^2 x}{(\log A)^2} + (\tfrac{7}{8})^x\,\frac{c_6 A^2}{\log A} < \frac{A^2}{4\log A}$$

for sufficiently large x, which is contrary to the prime number theorem.

We now consider an a_i for which the number of residues belonging to class 2 is greater than $\tfrac{7}{8}\phi(a_i)$.

Let these residues be $z_1, z_2, \ldots, z_l$; $l > \tfrac{7}{8}\phi(a_i)$. We denote by S_1 the number of solutions of the congruence $z_\kappa{}^2 + z_\lambda{}^2 \equiv 0 \pmod{a_i}$. In I we proved that

$$S_1 > \frac{2^{V(a_i)}\phi(a_i)}{16},$$

where $V(a_i)$ denotes the number of prime factors of a_i. Hence, by our lemma, the number of solutions of the congruence $p^2+q^2 \equiv 0 \pmod{a_i}$, with $p,\ q \leqslant A^2$, is greater than

$$\frac{2^{V(a_i)}\phi(a_i)\,A^4}{16\phi(a_i)^2(\log A)^4} > \frac{2^{V(a_i)}A^4}{16(\log A)^4 a_i} > \frac{2^{k/x}A^4}{32(\log A)^4 a_i} > \frac{2^{\log A/4x\log\log A}\,A^4}{32(\log A)^4 a_i}$$
$$> \frac{2^{\log A/5x\log\log A}\,A^4}{a_i},$$

since, by the prime number theorem for arithmetical progressions (or by a more elementary theorem),

$$k > \frac{\log A}{4\log\log A}.$$

---

* E. C. Titchmarsh, *Rend. di Palermo*, 54 (1930) 414–429.

But the integers of the form p^2+q^2, with $p, q < A^2$, are all less than $2A^4$. Hence there exists a multiple of a_i, say n, less than $2A^4$, for which the equation $n = p^2+q^2$ has more than

$$2^{(\log A/5x \log \log A)-1} > e^{\log A/10x \log \log A} = A^{1/10x \log \log A} > n^{1/50x \log \log A}$$

solutions; this concludes the proof.

2. The proof of the second theorem stated in the introduction is also similar to that of § 1 of I.

Let N be sufficiently large and let $A = 3.5 \dots p_\mu$, the product of the first μ odd primes such that $3 \dots p_\mu \leqslant N < 3 \dots p_\mu p_{\mu+1}$. We denote by ξ the number of r's not exceeding N, $\xi > N^{1-(c_4/\log \log n)}$, where $c_4 < \frac{1}{2}\log 2$, and estimate the number S of solutions of the congruence $r_j^2 - r_i^2 \equiv 0 \pmod{A}$ with $r_i < r_j \leqslant N$.

First we determine the number of different residue-classes mod A of the sequence $1^2, 2^2, 3^2, \dots, A^2$. It is well known that the number of different residue-classes mod p (p a prime) of the sequence $1^2, 2^2, \dots, p^2$ is equal to $\frac{1}{2}(p+1)$; hence, in consequence of the multiplicativity of residue-classes, the number of the different residue-classes mod A of the sequence $1^2, 2^2, \dots, A^2$ is equal to

$$z = \prod_{i=1}^{\mu} \tfrac{1}{2}(p_i+1) = \frac{A}{2^\mu} \prod_{i=1}^{\mu} \left(1+\frac{1}{p_i}\right).$$

Hence the residues mod A may be distributed into z classes such that the squares of the residues of each class are all congruent to one another mod A.

As in I, we denote by $y_1, y_2, \dots, y_z$ the numbers of r's not exceeding N and congruent to a residue of the 1st, 2nd, ... class. Thus we evidently have

$$S = \tfrac{1}{2}[y_1^2+y_2^2+\dots+y_z^2-y_1-y_2-\dots-y_z] = \tfrac{1}{2}[y_1^2+y_2^2+\dots+y_z^2] - \tfrac{1}{2}\xi,$$

since

$$y_1+y_2+\dots+y_z = \xi.$$

By a well-known elementary theorem, the sum of the squares of the y's is a minimum if they are all equal, *i.e.* if $y_i = \xi/z$; hence

$$S \geqslant \tfrac{1}{2}z\frac{\xi^2}{z^2} - \tfrac{1}{2}\xi = \tfrac{1}{2}\xi\left(\frac{\xi}{z}-1\right).$$

But

$$z = \frac{A}{2^\mu} \prod_{i=1}^{\mu}\left(1+\frac{1}{p_i}\right) < \frac{c_7 A \log \log A}{2^\mu} < \frac{A}{e^{c_8 \log A/\log \log A}} = A^{1-(c_8/\log \log A)}$$

for every $c_8 < \log 2$, since, by the prime number theorem,

$$\mu > c_9 \frac{\log \mathrm{A}}{\log \log A}$$

for every $c_9 < 1$ if A is sufficiently large. Thus

$$S \geqslant \tfrac{1}{2}\xi \left(\frac{\xi}{z} - 1\right) > \tfrac{1}{2}N^{1-(c_4/\log\log N)} \left(\frac{N^{1-(c_4/\log\log N)}}{A^{1-(c_8/\log\log A)}} - 1\right)$$

$$> \tfrac{1}{4}N^{1-(c_4/\log\log N)} \frac{N^{1-(c_4/\log\log N)}}{A^{1-(c_8/\log\log A)}} = \tfrac{1}{4}N^{1-(2c_4-c_8/\log\log N)} \frac{N^{1-(c_8/\log\log N)}}{A^{1-(c_8/\log\log A)}}$$

$$\geqslant \tfrac{1}{4}N^{1-(2c_4-c_8/\log\log N)}.$$

But $2c_4 < \log 2$; hence we may suppose that $c_8 > 2c_4$. Thus, finally,

$$S > \tfrac{1}{4}N^{1+(c_9/\log\log N)},$$

where $c_9 = c_8 - 2c_4 > 0$.

But the integers of the form $r_j^2 - r_i^2$ with $r_i < r_j \leqslant N$ are all positive and less than N^2, so that we can always find a multiple, say $M \leqslant N^2$, of A for which the equation $r_j^2 - r_i^2 = M$ has more than

$$\tfrac{1}{4}N^{c_9/\log\log N}\frac{A}{N} > \frac{1}{4p_{u+1}} N^{c_9/\log\log N} > M^{c_5/\log\log M}$$

solutions. Hence the result.

The University,
Manchester.

Printed by C. F. Hodgson & Son, Ltd., Newton St., London, W.C.2.